Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-14. **(Cancelled)**

15. **(Previously Presented)** The method of claim 34, wherein at least one of said operations in the first chain of operations comprises an exclusive OR.

16. **(Previously Presented)** The method of claim 34, wherein at least one of said operations in the first chain of operations comprises an operation of bit permutation of an intermediate result obtained from execution of an operation of said first chain of operations preceding said operation of bit permutation within said first chain of operations.

17. **(Previously Presented)** The method of claim 34, wherein at least one of said operations in the first chain of operations comprises an operation of indexed access to a table.

18. **(Previously Presented)** The method of claim 34, wherein at least one of said operations in the first chain of operations comprises an operation which is stable with respect to the application of an exclusive OR function.

19. **(Currently amended)** The method of claim 34, wherein at least one of said operations in the first chain of operations comprises an operation of transfer of an intermediate result obtained from execution of an operation of said ~~second~~ first chain of operations preceding said operation of transfer within said ~~second~~ first chain of operations, from one location to another one in a storage space.

20. **(Cancelled)**

21. **(Cancelled)**

22. **(Previously Presented)** The method of claim 34, wherein the step of randomly choosing comprises generating a random parameter that is used to identify which of said groups to choose, and wherein said method further comprises updating a complementation counter at each generation of the random parameter, and the selection in the step of outputting a resultant message to output the result of the last operation in either an uncompleted state or in a complemented state is made depending on a state of the complementation counter.

23. **(Previously Presented)** The method of claim 34, wherein the step of randomly choosing comprises generating a random parameter that is used to identify which of said groups to choose, and wherein said method further comprises updating, in parallel with each executed operation, information to be used during the step of outputting the resultant message to determine whether to output the result of the last operation in the uncomplemented state or the complemented state as the resultant message.

24. **(Previously Presented)** The method of claim 34, wherein the step of randomly choosing comprises a step of computing a parameter which is equal to a difference between a number of times when an operation of the first chain of operations is executed and a number of times when an operation of the second chain of operations is executed, and when the difference exceeds a given threshold, the step of randomly choosing is conducted so as to decrease the difference.

25. - 26. **(Cancelled)**

27. **(Currently amended)** The method of claim 34, wherein the step of storing, at the microcircuit card~~, a second set of instructions for a second chain of operations~~ comprises storing instructions for a succession of operations each corresponding to a complement byte by byte of ~~one~~ a respective ~~operation~~ one of the operations in the first chain of operations.

28. **(Currently amended)** The method of claim 34, wherein the step of storing, at the microcircuit card~~, a second set of instructions for a second chain of operations~~ comprises storing instructions for a succession of operations each corresponding to a complement bit by bit of ~~one~~ a respective ~~operation~~ one of the operations in the first chain of operations.

29. **(Currently Amended)**The method of claim 34, wherein the step of storing a second ~~step~~ set of instructions for the second chain of operations further comprises a step of applying a permutation of the order of successive commutative operations in the first chain of operations before storing said second ~~step~~ set of instructions.

30. **(Previously Presented)** The method of claim 29, wherein the step of determining a permutation of the order of successive commutative operations is carried out randomly.

31. **(Currently amended)** The method of claim 34, wherein the step of identifying comprises a step of determining the plurality of operations in said third group, ~~this~~ said step of determining ~~further~~ comprising generating a random parameter before ~~each~~ the random selection of ~~an~~ the operations ~~operation~~ from either the first chain of operations or from the second chain of operations and updating a complementation counter, and the step of outputting the resultant

message includes deciding to output the result of the last operation in the uncomplemented state or in the complemented state ~~depending of~~ depending on a state of the complementation counter.

32. **(Currently amended)** The method of claim 34, wherein the step of identifying comprises a step of determining the plurality of operations in said third group, ~~this~~ said step of determining ~~further~~ comprising generating a random parameter before ~~each~~ the random selection of an operation from either the first chain of operations or the second chain of operations and wherein said method further comprises updating, in parallel with each operation, information to be used during the step of outputting the resultant message to determine whether to output the result of the last operation in the uncomplemented state or the complemented state as the resultant message.

33. **(Currently amended)** The method of claim 34, wherein the step of identifying comprises a step of determining the plurality of operations in said third group, ~~this~~ said step of determining comprising a step of computing a parameter which is equal to a difference between a number of times when an operation of the first chain of operations is executed and a number of times when an operation of the second chain of operations is executed, and when the difference exceeds a given threshold, a next operation to be included in the selected chain of operations in said third group is selected from either the first chain of operations or the second chain of operations so as to decrease this difference.

34 **(Currently amended)** A method of executing and validating a cryptographic protocol between a server entity and a microcircuit card in order to

resist a DPA attack against the microcircuit card during execution of said cryptographic protocol, said method comprising the steps of:

storing a first set of instructions for a first chain of operations in both the server entity and the microcircuit card, said first chain of operations forming a data encryption method,

storing, at the microcircuit card, a second set of instructions for a second chain of operations based on the first chain of operations stored in said microcircuit card, said second chain of operations comprising a succession of operations each corresponding to a complement of ~~one~~ a respective ~~operation~~ one of the operations in the first chain of operations,

sending a message from said server entity to said microcircuit card,

executing, at the server entity, said first set of instructions for the first chain of operations stored therein using said message to obtain a server result,

identifying, in the microcircuit card, a selected chain of operations, said step of identifying comprising randomly choosing one of the following groups as said selected chain: 1) all of the operations in said first chain of operations; 2) all of the operations in said second chain of operations; or 3) a plurality of operations comprising a random selection of at least one of the operations in said first chain of operations and at least one of the operations in said second chain of operations, said plurality of operations comprising, for each operation of the first chain of operations, either ~~this~~ said operation or the respective operation in the second chain of operations corresponding to said operation,

executing, in the microcircuit card, instructions for the identified chain of operations on said message, outputting a result of a last operation executed in said identified chain of operations either in an uncomplemented state or a complemented state as a resultant message,

comparing the resultant message to the server result, and

validating the cryptographic protocol between the server entity and the microcircuit card when the server result and the resultant message are identical.

35. **(Cancelled)**